REMARKS

I. STATUS OF THE CLAIMS

In the Office Action mailed October 4, 2007, the Examiner noted that claims 27-43, 45 and 46 were pending and rejected claims 27-43 and 45-46. Claims 27, 28, 31-33, 36-43 and 45 have been amended, claim 46 has been canceled, no new claim has been added; and, thus, in view of the foregoing claims 27-43 and 45 remain pending for reconsideration which is requested. No new matter is believed to have been added. The Examiner's rejections are respectfully traversed below.

II. REJECTION OF CLAIM 45 UNDER 35 U.S.C. § 102(e) AS BEING ANTICIPATED BY KITAORI ET AL. (U.S. PATENT NO. 5,915,024)

Claim 45, as amended, recites

dividing data into a plurality of divisions;
applying a first function to all of said plurality of divisions using a first key to create
a first authenticator and applying a second function to all of said plurality of
divisions using a second key to create a second authenticator; and
appending linked authenticators, the linked authenticators being obtained by
linking the first and second authenticators, to the data

(claim 45, lines 2-7), which is supported by the embodiments of the invention on page 8, line 5 to page 9, line 7 of the Specification.

It is submitted that Kitaori fails to teach or suggest the above-mentioned features recited in claim 45. Rather, Kitaori is directed to an apparatus that adds an electronic signature to a document data (see Kitaori, Abstract). According to Kitaori, a delimiter character detector 2 has a function of detecting a predetermined delimiter character from the data text and dividing the data text into signature message each having a delimiter character at the end of the message and an appropriate length (see Kitaori, col. 7, lines 24-28). Further, according to Kitaori, a digest generator 4 applies a hash function 6 to the signature message (containing the divided document information) to generate a message digest (see Kitaori, col. 8, lines 5-7), and an encrypter 8 encrypts the digest using the self secret key stored in the secret key memory 10 (see Kitaori, col. 8, lines 19-20). As a result, the signature-added message generator 12 adds the electric signature thus obtained to the signature message (see Kitaori, col. 8, lines 33-34 and Fig.4).

However, Kitaori fails to teach or suggest "applying a first function to all of a plurality of divisions using a first key to create a first authenticator and applying a second function to all of the plurality of divisions using a second key to create a second authenticator" as recited in claim

45 because, according to Fig. 4 of Kitaori, each electric signature is generated from a single signature message respectively.

Therefore, the Applicants respectfully submit that claim 45 patentably distinguishes over Kitaori. Accordingly, Applicants respectfully request that the rejection be withdrawn.

III. REJECTION OF CLAIMS 27, 32, 37-43 AND 45 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER KITAORI ET AL. IN VIEW OF OLARIG ET AL. (U.S. PATENT NO. 6,009,524)

Claim 27, as amended, recites

a dividing unit which divides the information into the plurality of data divisions;
an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and
an appending unit which links the first and second authenticators, and appends linked authenticators to the information for sending with the information to a certifying apparatus in the authentication system

(claim 27, lines 4-11).

Claim 37 and 39, as amended, recite

dividing the information into the plurality of data divisions;
creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;
creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and
appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the information for sending with the information to a certifying apparatus in the authentication system

(claim 37, lines 4-11 and claim 39, lines 6-13).

Claim 45, as amended, recites

dividing data into a plurality of divisions, applying a first function to all of said plurality of divisions using a first key to create a first authenticator and applying a second function to all of said plurality of divisions using a second key to create a second authenticator, and appending linked authenticators, the linked authenticators being obtained by linking the first and second authenticators, to the data

(claim 45, lines 2-7). Support for claim amendments can be found on page 8 line 5 to page 9 line 24 of the Specification.

It is submitted that Kitaori does not teach or suggest the above-mentioned features of claims 27, 37, 39 and 45. Rather, Kitaori is directed to an apparatus that adds an electronic signature to a document data (see Kitaori, Abstract). According to Kitaori, a delimiter character

detector 2 detects a predetermined delimiter character from the data text and divides the data text into signature message each having a delimiter character at the end of the message and an appropriate length (see Kitaori, col. 7, lines 24-28). Further, according to Kitaori, a digest generator 4 applies a hash function 6 to the signature message (containing the divided document information) to generate a message digest (see Kitaori, col. 8, lines 5-7), and an encrypter 8 encrypts the digest using the self secret key stored in the secret key memory 10 (see Kitaori, col. 8, lines 19-20). As a result, the signature-added message generator 12 adds the electric signature thus obtained to the signature message (see Kitaori, col. 8, lines 33-34, and Fig. 4).

However, Kitaori fails to teach or suggest "creating a first authenticator by applying a first one-way function using a first key to all of the data divisions" and "creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different" as recited in claim 37, for example, because, according to Fig. 4 of Kitaori, each electric signature is generated from a single signature message respectively.

Olarig describes an upgrade software having a first digital signature attached using a vendor's private key and the second digital signature attached using a vendor's private key (see Olarig, col. 4, lines 1-54). Therefore, Olarig also fails to teach or suggest the above-mentioned features recited in claims 27, 37, 39 and 45.

Therefore, even if one were to combine the disclosure of these cited references, the resulting combination would not disclose "creating a first authenticator by applying a first one-way function using a first key to all of the data divisions" and "creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different".

In order to form a proper § 103(a) rejection, the cited references must combine to disclose or suggest all of the cited features of the rejected claim. Therefore, as none of the cited references, taken alone or in combination, disclose or suggest at least the above feature of claims 27, 37, 39 and 45 of the invention. Thus, the Applicants respectfully submit that claims 27, 37, 39 and 45 patentably distinguish over the cited references.

Claim 32, as amended, recites

a separating unit which separates out the information and linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;
a dividing unit which divides the information separated out by the separating unit

into the plurality of data divisions;
an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator of the linked authenticators separated out by the separating unit, and by comparing the second authenticator with a fourth authenticator of the linked authenticators separated out by the separating unit

(claim 32, lines 4-16).

Claim 38 and 40, as amended, recite

separating out the information and linked authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;
dividing the separated out information into the plurality of data divisions;
creating a first authenticator by applying a first one-way function using a first key to all of the data divisions;
creating a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different; and
authenticating the information by comparing the first authenticator with a third authenticator of the linked authenticators, and by comparing the second authenticator with a fourth authenticator of the linked authenticators

(claim 38, lines 4-13 and claim 40, lines 6-15). Support for claim amendments can be found on page 8, line 5 to page 9, line 24 of the Specification.

It is submitted that neither Kitaori nor Olarig, taken alone or in combination, teach or suggest the above-mentioned features as recited in claims 32, 38 and 40. Rather, Kitaori is directed to an apparatus that adds an electronic signature to a document data (see Kitaori, Abstract). According to Kitaori, the signature divider 22 extracts a set of signature message and electric signature from a signature-added message (see Kitaori, col. 9, lines 63-65), the digest generator 24 applies a hash function to the extracted signature messages (see Kitaori, col. 10, lines 26-32), and comparator 32 compares digests (see Kitaori, col. 10, lines 36-41).

According to Olarig, each of the digital signatures is verified using the stored public keys (see Olarig, col. 4, lines 16-20).

However, Kitaori and Olarig fail to teach or suggest "creating a first authenticator by applying a first one-way function using a first key to all of the data divisions" and "creating a second authenticator by applying a second one-way function using a second key to all of the data divisions".

Therefore, even if one were to combine the disclosure of these cited references, the resulting combination would not disclose "creating a first authenticator by applying a first one-

12

way function using a first key to all of the data divisions" and "creating a second authenticator by applying a second one-way function using a second key to all of the data divisions".

As none of the cited references, taken alone or in combination, disclose or suggest at least the above feature of claims 32, 38 and 40 of the invention. Thus, the Applicants respectfully submit that claims 32, 38 and 40 also patentably distinguish over the cited references.

Claim 41 recites similar features as claims 27 and 32 which are not disclosed or suggested by the cited references. Claim 42 recites similar features as claims 37 and 38 which are not disclosed or suggested by the cited references. Claim 43 recites similar features as claims 39 and 40 which are not disclosed or suggested by the cited references. Therefore, the Applicants respectfully submit that claims 41-43 also patentably distinguish over the cited references.

Accordingly, Applicants respectfully request that the rejection be withdrawn.

IV. REJECTION OF CLAIMS 28 AND 33 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER KITAORI ET AL. IN VIEW OF OLARIG ET AL. IN VIEW OF HERBERT ET AL. (U.S. PATENT NO. 6,023,509)

Claim 28 depends from claim 27, and includes features of claim 27 which are not disclosed or suggested by Kitaori or Olarig.

Herbert is related to encoding a purpose into a digital signature, where the purpose and digital signature are bound into an extended digital signature (see Herbert, Abstract). According to Herbert, a next 512-bit segment of input data is used with the output hash value of the previous segment as the input data to create another hash value (see Herbert, col. 3, lines 19-21). However, Herbert fails to disclose or suggest "an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different".

Therefore, the Applicants respectfully submit that claim 28 also patentably distinguishes over the cited references

Claim 33 depends from claim 32, and includes features of claim 32 which are not disclosed or suggested by Kitaori or Olarig. Herbert also fails to disclose or suggest "an authenticator creating unit which creates a first authenticator by applying a first one-way function

using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions".

Therefore, the Applicants respectfully submit that claim 33 also patentably distinguishes over the cited references

Accordingly, Applicants respectfully request that the rejection be withdrawn.

V.   REJECTION OF CLAIMS 29, 31, 34 AND 36 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER KITAORI ET AL. IN VIEW OF OLARIG ET AL. IN VIEW OF DOLAN ET AL. (U.S. PATENT NO. 5,604,801)

Claim 29 depends from claim 27, and includes features of claim 27 which are not disclosed or suggested by Kitaori or Olarig. Claim 29 recites "the appending unit appends authenticators obtained by truncating the first and second authenticators to the information".

Claim 31 depends from claims 27 and 28 and includes features of claims 27 and 28 which are not disclosed or suggested by Kitaori or Olarig. Claim 31 recites "intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as the second initial value to create the second authenticator".

Claim 34 depends from claim 32, and includes features of claim 32 which are not disclosed or suggested by Kitaori or Olarig. Claim 34 recites "separating unit obtains truncated authenticators from the data received from the signing apparatus, and the certifying unit compares an authenticator obtained by truncating the first authenticator with the truncated third authenticator separated out by the separating unit, and compares an authenticator obtained by truncating the second authenticator with the truncated fourth authenticator separated out by the separating unit".

Claim 36 depend from claims 32 and 33, and includes features of claims 32 and 33 which are not disclosed or suggested by Kitaori or Olarig. Claim 36 recites "intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as the second initial value to create the second authenticator".

Dolan is related to a public key data communications system under control of a portable security device (see Dolan, Abstract). According to Dolan, a digital signature is generated from the message by first generating a hash value of the message using a strong hash function and then encrypting the hash value using the secret key (see Dolan, col. 6, lines 1-12). However, Dolan fails to disclose or suggest "truncating the first and second authenticators", "the certifying unit compares an authenticator obtained by truncating the first authenticator with the truncated

third authenticator", and "intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as an initial value to create the second authenticator".

Therefore, the Applicants respectfully submit that claims 29, 31, 34 and 36 also patentably distinguish over the cited references.

Accordingly, Applicants respectfully request that the rejection be withdrawn.

VI. REJECTION OF CLAIMS 30 AND 35 UNDER 35 U.S.C. § 103(a) AS BEING UNPATENTABLE OVER KITAORI ET AL. IN VIEW OF OLARIG ET AL. IN VIEW OF BELLARE ET AL. (U.S. PATENT NO. 5,757,913)

Claim 30 depends from claim 27 and includes features of claim 27 which are not disclosed or suggested by Kitaori or Olarig.

Bellare is related to a system that provides data authentication within a data communication environment, which is simple, fast and secure (see Bellare, Abstract). According to Bellare, authentication codes are created and verified in such a way that the operations can be performed in parallel, or pipelined, fashion (see Bellare, col. 1, lines 60-65). However, Bellare also fails to disclose or suggest "an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions, where the first and second keys are different".

Therefore, the Applicants respectfully submit that claim 30 also patentably distinguishes over the cited references.

Claim 35 depends from claim 32 and includes features of claim 32 which are not disclosed or suggested by Kitaori or Olarig. Bellare also fails to disclose or suggest "an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to all of the data divisions, and creates a second authenticator by applying a second one-way function using a second key to all of the data divisions".

Therefore, the Applicants respectfully submit that claim 35 also patentably distinguishes over the cited references.

Accordingly, Applicants respectfully request that the rejection be withdrawn.

VII.   CONCLUSION

In accordance with the foregoing, it is respectfully submitted that all outstanding objections and rejections have been overcome and/or rendered moot. Further, all pending claims patentably distinguish over the prior art. There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If any further fees, other than and except for the issue fee, are necessary with respect to this paper, the U.S.P.T.O. is requested to obtain the same from deposit account number 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 3/4/2008   By: _____

                                  Sheetal S. Patel
                                  Registration No. 59,326

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501